

**CSR** Cyber  
Security  
Raad

# JAAROVERZICHT 2017





# VOORWOORD

Nederland bevindt zich in de voorhoede als het gaat om digitalisering. Nederland moet een veilig, open en welvarende samenleving zijn en blijven en dat vraagt onze structurele aandacht. Onze digitale weerbaarheid blijft achter bij de groei van dreigingen. Overheid, bedrijfsleven en burgers nemen veel stappen om de digitale weerbaarheid te vergroten, maar dit gaat niet snel genoeg. We moeten de komende jaren actief en harder blijven werken om de vooraanstaande positie te behouden en de economische kansen die een digitaal veilige economie biedt, te verzilveren. Alleen zo kunnen we de digitale weerbaarheid van Nederland vergroten. De Cyber Security Raad (CSR) heeft hier het afgelopen jaar actief op ingezet.

Het jaar 2017 begon voor de raad met de uitkomsten van de evaluatie van de CSR. De raad werd eind 2011 opgericht en is na vijf jaar geëvalueerd. Uit de evaluatie blijkt dat de raad als een zinvol strategisch adviesorgaan wordt ervaren met een unieke samenstelling (publiek, privaat én wetenschappelijk). Ook blijkt dat de raad meer impact zou kunnen hebben door scherper te adviseren. De uitkomsten van het evaluatieonderzoek vormen de basis voor CSR Nieuwe Stijl. De raad spreekt de ambitie uit om scherpere adviezen uit te brengen met een heldere boodschap en een duidelijke adressering. Daarbij blijft de raad zich onafhankelijk en kritisch opstellen naar alle spelers in het cybersecurityveld. Dit leidt soms tot 'spannende' adviezen, bijvoorbeeld omdat een advies vooruitloopt op ontwikkelingen binnen de EU of omdat er verschillende belangen tegen elkaar moeten worden afgewogen. Om aan kracht en snelheid te winnen is bij het formuleren van standpunten volledige consensus binnen de raad geen randvoorwaarde. Het gaat erom dat we stappen vooruit kunnen zetten en Nederland in de voorhoede houden.

Het afgelopen jaar heeft dit tot mooie resultaten geleid, zoals de publicatie van de handreiking zorgplichten die bedrijven beter inzicht biedt in de complexe wet- en regelgeving rondom zorgplichten. Ook heeft de raad zich ingezet om het midden- en kleinbedrijf middels een landelijk dekkend stelsel van informatieknooppunten in een betere informatiepositie te stellen door ze te voorzien van dreigingsinformatie en advies hoe te handelen. Dit heeft er mede toe bijgedragen dat in 2018 het nieuwe Digital Trust Centre (DTC) van start gaat. De CSR heeft eveneens een advies voorbereid om de uitdagingen die het Internet of Things met zich meebrengt het hoofd te bieden. Dit advies is in januari 2018 afgerond en overhandigd aan het kabinet en VNO/NCW.

Het jaar 2017 was ook het jaar waarin een nieuw kabinet is geformeerd. Uit het nieuwe regeerakkoord blijkt het belang van cybersecurity; er wordt structureel 95 miljoen euro gereserveerd, verdeeld over verschillende departementen. Een mooie start voor het nieuwe jaar waarin we verder kunnen werken aan het vergroten van de digitale weerbaarheid in ons land. Dat is immers waar we voor staan!



# 1. CYBER SECURITY RAAD

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en het bedrijfsleven (via het kabinet) en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in ons land te verhogen. Nederland wil een open, veilig en welvarende samenleving zijn, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd. De CSR draagt bij aan deze ambitie door vooruit te kijken en te signaleren wat er op Nederland afkomt en ook te adviseren over wat er in Nederland zou moeten gebeuren. In 2011 heeft de toenmalige minister van Veiligheid en Justitie de CSR geïnstalleerd.

## Taakstelling

De raad heeft drie taken die bijdragen aan het behalen van de missie:

1. Het gevraagd en ongevraagd verstrekken van strategisch advies over cybersecurity aan het kabinet en het bedrijfsleven (via het kabinet).
2. Het volgen van trends en nieuwe technologische ontwikkelingen en deze waar nodig vertalen in strategische adviezen over mogelijke maatregelen om de risico's voor cybersecurity te verkleinen en de economische kansen te vergroten.
3. Het initiëren en/of versnellen van relevante initiatieven binnen Nederland en de Europese Unie die een aantoonbare bijdrage leveren aan het verhogen van het cybersecurityniveau in Nederland.

## Samenstelling

De samenstelling van de CSR is gerelateerd aan de in de programmering geformuleerde doelstellingen. De raad streeft naar een zo breed mogelijke dekking van invalshoeken op het terrein van cybersecurity. Daarom hebben achttien leden zitting volgens de verdeelsleutel 7-7-4: zeven leden uit de private sector, zeven leden uit de publieke sector en vier leden uit de wetenschap. De CSR heeft twee covoorzitters: één namens de publieke sector en één namens de private sector. De leden vertegenwoordigen een relevante organisatie of sector binnen het cybersecuritydomein. De leden worden volgens een vastgestelde procedure benoemd.

De unieke samenstelling (publiek, privaat en wetenschap) maakt het mogelijk prioriteiten, knelpunten en kansen vanuit diverse invalshoeken te benaderen. Door deze onafhankelijkheid en kritische blik houdt de raad de Nederlandse aanpak voor cybersecurity scherp en levert zo een wezenlijke bijdrage aan een veilig, open en welvarende samenleving. De standpunten van de CSR winnen door deze brede samenstelling aan kracht.

## Werkwijze

De CSR komt vier keer per jaar bijeen in een plenaire vergadering. De leden van de CSR worden ter voorbereiding op deze vergaderingen ondersteund door ondersteuners vanuit hun eigen organisatie.



“De afgelopen jaren hebben we gezien welke impact digitale aanvallen op de samenleving hebben. De ontwikkelingen in het digitale domein bieden ontzettend veel kansen, maar die kunnen we alleen volop benutten als we onze digitale veiligheid op orde hebben. Daarom heeft het nieuwe kabinet 95 miljoen euro extra uitgetrokken om te investeren in cybersecurity. In het voorjaar van 2018 zal ik de Nederlandse Cybersecurity Agenda presenteren. Uiteraard zullen belangrijke onderwerpen waar de Cyber Security Raad de afgelopen maanden over heeft geadviseerd, zoals het Internet of Things en informatiedeling daar een prominente plek in krijgen. Alleen samen kunnen we Nederland digitaal veilig houden. Daarin heeft de Cyber Security Raad een belangrijke rol. Het ministerie hecht veel waarde aan de verbinding tussen publiek, privaat en wetenschap zoals in de raad plaatsvindt.”

*Ferd Grapperhaus, minister Justitie en Veiligheid*

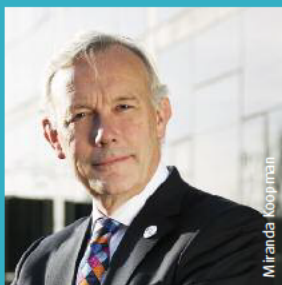
Naast de plenaire vergadering heeft de CSR een aantal subcommissies benoemd die zich richten op meer specifieke onderwerpen. In de subcommissies hebben raadsleden zitting en ook hierbij is de samenstelling publiek, privaat en wetenschappelijk. De subcommissies diepen onderwerpen uit, al dan niet ondersteund door een werkgroep en/of een wetenschappelijk onderzoek.

De CSR levert verschillende type producten op. Zo stelt de raad adviezen en handreikingen op, voeren individuele leden boardroomgesprekken bij organisaties en bedrijven, zet de raad onderzoeken uit bij onderzoekers en initieert de raad verschillende activiteiten, zoals in het afgelopen jaar het Cyber Security debat, Symposium CSR en iBestuur, (mini-) seminar Internet of Things en de tweede editie van de National Cyber Security Summer School.



# 2. SAMENSTELLING

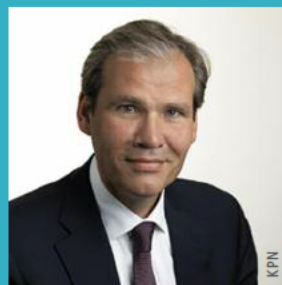
## PRIVATE SECTOR



**Dhr. J. (Jos) Nijhuis RA**  
(covoorzitter)  
CEO Schiphol Group, lid van  
CSR namens VNO-NCW



**Mw. mr. I. (Ineke) Dezentjé  
Hamming-Bluemink**  
voorzitter FME (onder-  
nemersorganisatie voor de  
technologische industrie),  
lid van de CSR namens FME



**Dhr. mr. J.F.E. (Joost)  
Farwerck**  
Lid Raad van Bestuur en COO  
KPN, lid van CSR namens  
Nederland ICT



**Dhr. M. (Marcel) Krom**  
CIO PostNL, lid van CSR  
namens CIO Platform



**Mw. T. (Tineke)  
Netelenbos**  
Voorzitter ECP, platform voor  
de informatiesamenleving



**Dhr. ir. B.G.M. (Ben)  
Voorhorst**  
COO TenneT, lid van CSR  
namens de vitale sectoren



**Dhr. drs. R. (Ruben)  
Wenselaar**  
Voorzitter van de Raad van  
Bestuur van Menzis en be-  
stuurslid Zorgverzekeraars  
Nederland (ZN), lid van de  
CSR namens de zorgsector

## PUBLIEKE SECTOR



**Dhr. drs. H.W.M. (Dick)  
Schoof**  
(covoorzitter)  
Nationaal Coördinator  
Terrorismebestrijding en  
Veiligheid



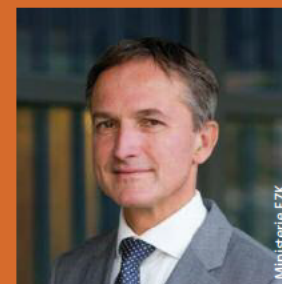
**Mw. J. (Jannine) van den  
Berg**  
Politiechef van de Landelijke  
Eenheid bij de Nationale  
Politie



**Dhr. R.A.C. (Rob) Bertholee**  
Directeur-Generaal  
Algemene Inlichtingen- en  
Veiligheidsdienst (AIVD)



**Dhr. mr. G.W. (Gerrit) van  
der Burg**  
Voorzitter van het College  
van procureurs-generaal



**Dhr. mr. A.F. (Sandor)  
Gaastra**  
Directeur-generaal Energie,  
Telecom en Mededinging  
bij het ministerie van  
Economische Zaken en  
Klimaat



**Dhr. dr. S.J.G. (Sebastian)  
Reyn**  
Directeur Strategie, Beleids-  
ontwikkeling en Innovatie bij  
het ministerie van Defensie

### Teruggetreden in 2017

Dhr. drs. E. (Eelco) Blok, (voormalig  
covoorzitter namens de private sector)  
Voorzitter Raad van Bestuur en CEO van  
KPN, lid van CSR namens VNO-NCW  
Dhr. drs. H.B. (Bas) Eenhoorn, Nationaal  
Commissaris Digitale Overheid  
Dhr. drs. J.C. (Jos) de Groot, Directeur  
Telecommarkt bij het directoraat-generaal  
Energie, Telecom en Mededinging bij het  
ministerie van Economische Zaken  
(waarnemend)  
Dhr. R. (Ron) de Mos, Senior Vice President  
en General Manager CGI Nederland, lid van  
CSR namens Nederland ICT

## WETENSCHAPPELIJKE SECTOR



**Mw. prof. dr. B. (Bibi) van  
den Berg**  
Hoogleraar Cybersecurity  
Governance verbonden aan  
het Institute of Security  
and Global Affairs van  
Universiteit Leiden



**Dhr. prof. dr. M.J.G.  
(Michel) van Eeten**  
Hoogleraar Cybersecurity  
TU Delft



**Dhr. prof. dr. B.P.F. (Bart)  
Jacobs**  
Hoogleraar Computer-  
beveiliging Radboud  
Universiteit Nijmegen



**Mw. prof. mr. E.M.L.  
(Lokke) Moerel**  
Senior Of Counsel Morrison  
& Foerster LLP, Hoogleraar  
Global ICT Law Universiteit  
Tilburg

## BUREAU CSR



**Mw. drs. E.C. (Elly) van den  
Heuvel**  
Secretaris

**Mw. drs. A.A. (Andrea) Bakker**  
Adjunct-secretaris

**Mw. H.M. (Heidi) Letter**  
Communicatieadviseur

**Dhr. S.L.J. (Siep) van Sommeren**  
Beleidsmedewerker

**Mw. M. (Martine) Spaans**  
Beleidsondersteuner

**Dhr. L. (Lars) van Zijl**  
Stagiair

**Vertrokken:**  
**Dhr. M.N. (Martin) Bobeldijk**  
Communicatieadviseur

### Toegetreden in 2017

**Mw. mr. I. (Ineke) Dezentjé Hamming-  
Bluemink**, voorzitter FME  
(ondernemersorganisatie voor de  
technologische industrie), lid van de CSR  
namens FME  
**Dhr. mr. J.F.E. (Joost) Farwerck**, Lid Raad van  
Bestuur en COO KPN, lid van CSR namens  
Nederland-ICT  
**Dhr. drs. R. (Ruben) Wenselaar**, Voorzitter  
van de Raad van bestuur van Menzis en  
bestuurslid Zorgverzekeraars Nederland  
(ZN), lid van de CSR namens de zorgsector  
**Dhr. mr. A.F. (Sandor) Gaastra**, Directeur-  
generaal Energie, Telecom en Mededinging  
bij het ministerie van Economische Zaken en  
Klimaat



# 3. WERKPROGRAMMA

De Cyber Security Raad (CSR) is in het afgelopen jaar met een viertal strategische thema's aan de slag gegaan. De thema's zijn toekomstgericht, hebben een maatschappelijke en economische relevantie en hangen nauw met elkaar samen. Alle onderwerpen dragen bij aan het versterken van de cybersecurity van Nederland en vormden in 2017 de leidraad voor de agendering van de raad. De onderwerpen zijn al dan niet uitgediept in subcommissies.

De onderwerpen waartoe de raad in 2017 verschillende producten en adviezen voor heeft ontwikkeld of zich op een andere wijze voor heeft ingezet, zijn:

- Zorgplichten
- Onderwijs
- Internet of Things
- Informatie-uitwisseling en cybersecurity en cybercrime

## Zorgplichten

Volgens de huidige wet- en regelgeving hebben bedrijven de plicht om te zorgen voor een adequate digitale beveiliging. Mocht zich toch een incident voordoen, dan hebben zij de plicht de gevolgen ervan te beperken en verdere incidenten te voorkomen. In de praktijk blijkt dat bedrijven hier onvoldoende van op de hoogte zijn. Dat kan er bijvoorbeeld toe leiden dat bedrijven hun systemen onvoldoende beveiligen en er producten op de markt worden gebracht die onvoldoende tegen hacken zijn beveiligd. Door nieuwe technologische ontwikkelingen, zoals Internet of Things en eHealth, neemt het risico op digitale én fysieke schade sterk toe.

In april 2017 heeft de CSR een [advies](#) en een handreiking aangeboden aan het kabinet (voormalige ministeries van Veiligheid en Justitie en Economische Zaken) en aan VNO-NCW. De raad heeft het kabinet geadviseerd zelfregulering ten aanzien van 'zorgplichten' te stimuleren, het voortouw te nemen in een discussie hierover, en de wetgeving van Europese lidstaten op elkaar af te stemmen. VNO-NCW heeft het advies gekregen om met haar leden over dit onderwerp in gesprek te gaan en invulling te geven aan de verplichte zorg voor digitale veiligheid. [De publicatie 'Ieder bedrijf heeft zorgplichten', handreiking voor bedrijven op gebied van cybersecurity'](#) is op de website van de CSR beschikbaar. De handreiking, die door het bureau secretariaat van de CSR en door VNO-NCW is verspreid onder bedrijven, bevat onder andere een overzicht van de





belangrijkste juridische zorgplichten voor bedrijven op het gebied van cybersecurity en de belangrijkste handvatten om deze plichten in te vullen. Diverse topjuristen, Radboud Universiteit, Openbaar Ministerie, Nederland ICT, CIO Platform Nederland en Consumentenbond hebben hieraan meegewerkt. Nederland ICT en het CIO Platform Nederland hebben aangegeven hun achterban te willen assisteren bij de implementatie van de handreiking.

## Onderwijs

### Voortgang advies 'Cybersecurity in het onderwijs en bedrijfsleven'

In 2015 heeft de CSR het [advies inzake 'Cybersecurity in het onderwijs en het bedrijfsleven'](#) aangeboden aan de toenmalige staatssecretarissen van Veiligheid en Justitie en Onderwijs, Cultuur en Wetenschap. In 2016 heeft er een gesprek plaatsgevonden tussen de CSR en de staatssecretaris van Onderwijs, Cultuur en Wetenschap. In 2017 heeft de raad zich ingezet om de impact van het advies te stimuleren. De raad is hiervoor in gesprek gegaan met respectievelijk het ministerie van OCW en curriculum.nu (tijdelijke organisatie die werkt aan de herziening van het landelijk curriculum in het primair en voortgezet onderwijs). Doel van het gesprek was om de mogelijkheden te verkennen om opvolging te geven aan de afspraak die is

gemaakt om met kennis en kunde bij te dragen aan de invulling van het vak 'digitale geletterdheid' in het nieuwe curriculum naar aanleiding van het advies 2032 (onder leiding van Paul Schnabel). In het proces van de curriculumwijziging zijn er in 2018 verschillende momenten om met kennis en kunde vanuit het bedrijfsleven en initiatieven/lesprogramma's op het terrein van cybersecurity bij te dragen.

### National Cyber Security Summer School (NCS3)

De NCS3 is een initiatief van de CSR naar aanleiding van het advies 'Cybersecurity in onderwijs en bedrijfsleven'. In 2017 vond de tweede editie plaats, georganiseerd door dcypher in samenwerking met CGI, Nederland ICT, Nationaal Cyber Security Centrum (NCSC) en nog een aantal andere enthousiaste partners. De studenten kregen les van cybersecurity-experts van universiteiten, uit het bedrijfsleven en van de overheid. De NCS3 biedt hen de mogelijkheid om kennis te maken met de cybersecurity en de aspecten ervan en meer te leren over het belang van samenwerking op dit vlak tussen publieke, private en wetenschappelijke partijen.

Onderdeel van de NCS3 is de CSR Challenge. De studenten strijden tijdens deze challenge om een beleidsadvies aan de CSR te mogen geven. In 2017 stond de CSR Challenge in het teken van inzet nieuwe technologieën. Alle deelnemende studenten hebben zich in groepen gebogen over de vraag hoe we in Nederland nieuwe technologieën in kunnen zetten voor de cybersecurity van de Nederlandse vitale







sectoren. De groep met het beleidsadvies 'Toepassing blockchain in de voedings- en landbouwsector' heeft de challenge gewonnen. Het winnende team heeft het advies gepresenteerd tijdens de CSR raadsvergadering in september 2017. De leden van het winnende team kregen tevens de mogelijkheid om hun voorkeuren voor een stageplaats bij verschillende organisaties in Nederland kenbaar maken.

### Internet of Things

In het afgelopen jaar heeft de CSR een advies voorbereid om Internet of Things (IoT) op verantwoorde wijze te laten landen in onze samenleving. Dit [advies](#) volgt op het onderzoek naar de belangrijkste vraagstukken rondom IoT dat de CSR in 2016 heeft laten uitvoeren.

Aanleiding voor het CSR advies is het besef dat als er geen maatregelen worden genomen het IoT ingrijpende gevolgen kan hebben in de fysieke en digitale wereld en

daarmee voor de digitale toppositie van Nederland. Het is van belang dat de veiligheids- en privacyrisico's worden aangepakt om schade zoveel mogelijk te beperken en voorkomen. Om te kunnen profiteren van de kansen die het IoT biedt, moet er tevens op een veilige manier ruimte worden geboden voor nieuwe ontwikkelingen en innovatie. Daarvoor is gerichte actie nodig van onder andere de ministeries van Economische Zaken en Klimaat, Justitie en Veiligheid en Binnenlandse Zaken en Koninkrijksrelaties.

### (Mini-)Seminar Internet of Things

In november 2017 vond op initiatief van de CSR een besloten (mini-)seminar plaats met als thema 'Internet of Things'. De genodigden voor deze avond waren CEO's, bestuurders en topmanagers uit de publieke, private én wetenschappelijke sector, waaronder afgevaardigden van ministeries, topbestuurders/-managers, wetenschappers, CEO's van bedrijven en instellingen, een aantal studenten van de NCS3 en raadsleden van de CSR. Aanleiding voor het seminar was het afscheid van de heer drs. Eelco Blok als covoorzitter van de raad.





Het seminar werd geopend door de minister van Justitie en Veiligheid, prof. mr. F.B.J. (Ferdinand) Grapperhaus. Hij bedankte de heer Eelco Blok persoonlijk voor zijn inzet als covoorzitter van de CSR in de afgelopen jaren. Sinds de oprichting van de raad in 2011 is Eelco Blok covoorzitter van de Raad geweest. Aansluitend werden tijdens het seminar inhoudelijke bijdragen verzorgd door prof. dr. ing. Dave Blank, nanotechnoloog en nanotech futurist, ir. Gilles Ampt CISM CIPP/E, voorzitter van de Security Community Smart Mobility en dr. Paul Timmers, onafhankelijk adviseur voor digitale innovatie en voormalig directeur van de Europese Commissie voor Digital Society, Trust & Cybersecurity. Van alle bijdragen en opbrengsten tijdens de avond is een [verslag](#) gemaakt met daarin een overzicht van de belangrijkste conclusies op de stellingen van de sprekers. De CSR neemt de uitkomsten hiervan waar mogelijk mee in zijn toekomstige activiteiten.

### Informatie-uitwisseling en cybersecurity en cybercrime

Het tijdig beschikken over de juiste informatie is van groot belang voor de digitale weerbaarheid van organisaties, publiek én privaat. Het bedrijfsleven dat als niet vitaal staat aangemerkt heeft bewust of onbewust een ernstig informatiekort. Dit komt omdat zij onvoldoende of niet zijn aangesloten op de structuur waarbinnen informatie over cybersecurity wordt gedeeld. Deze bedrijven vormen daardoor een makkelijk doelwit voor cybercriminelen. Een goede landelijke informatievoorziening helpt de weerbaarheid van Nederland te verhogen.

Om die reden heeft de CSR in juli 2017 het [advies 'Naar een landelijk dekkend stelsel van informatieknooppunten'](#) gepubliceerd. Daarin adviseert de raad om ook het niet-vitale deel van het bedrijfsleven te voorzien van dreigingsinformatie en advies hoe te handelen en wordt gepleit voor een snelle komst van een Digital Trust Centre (DTC). Ook heeft de raad geadviseerd een financiële stimulans voor brancheorganisaties mogelijk te maken, zodat brancheorganisaties een functie op het terrein van cybersecurity richting het bedrijfsleven kunnen vervullen. De raad adviseert eveneens het inzicht in cybercrime te vergroten door het stimuleren van het doen van meldingen en het versterken van de publiek-private samenwerking op dit terrein. Het advies is aangeboden aan meerdere partijen, waaronder de toenmalige minister van Economische Zaken, de toenmalige staatssecretaris van Veiligheid en Justitie, de Korpschef Nationale Politie en het College van procureurs-generaal. Daarnaast was het advies was ook geadresseerd aan de voorzitters van VNO-NCW, MKB-Nederland, Nederland ICT, CIO Platform Nederland, Kamer van Koophandel en de brancheverenigingen.

### CSR Magazine

In maart 2017 is de [derde editie van het CSR Magazine](#) verschenen. Het is een speciale uitgave over de economische en maatschappelijke noodzaak van meer cybersecurity. Meerdere topfunctionarissen uit overheid en bedrijfsleven spreken zich in het magazine uit over wat er nodig is om Nederland digitaal veiliger te krijgen én over het economische belang daarvan. Nederland heeft een digitaal Deltaplan nodig. Dankzij visie, ambitie, actie en budget houdt Nederland droge voeten. Een dergelijke aanpak is ook nodig om digitaal droge voeten te houden en het cybersecurityniveau in Nederland te verhogen. Niets doen is geen optie.

Er doen zich grote economische kansen voor, is een gedeelde mening van veel auteurs in het CSR Magazine. Nederland kan gidsland zijn in de wereld op het gebied van cybersecurity. Net als watermanagement kan cybersecurity een onderwerp zijn waarop Nederland het verschil kan maken. Er is veel kennis voorhanden, maar versnipperd. Door een betere kennisuitwisseling en door te investeren in innovatieve producten en diensten kan Nederland internationaal een leidende rol blijven vervullen op het gebied van cybersecurity. Politiek, overheid, bedrijfsleven en kennisinstituten zijn aan zet.





# 4. INTERNATIONAAL

Samenwerking op internationaal niveau als het gaat om cybersecurity is en blijft van groot belang. Geen enkel land kan de vraagstukken rondom cybersecurity zelfstandig oplossen. De vraagstukken hebben een grensoverschrijdend karakter. Ook hier heeft de Cyber Security Raad (CSR) zich in 2017 voor ingezet.

## Stimulering oprichting Cyber Security Raden binnen de EU

In het kader van kennisdeling tussen de EU-lidstaten stimuleert de CSR de oprichting van gelijksoortige raden met publiek-privaat-wetenschappelijke samenstelling in andere EU-landen. Verschillende lezingen zijn gegeven door de secretaris van de raad.

## IGF Geneve

Tijdens het IGF in Genève organiseerde de CSR een Open Forum over zorgplichten en het Internet of Things (IoT). Het doel was een discussie over de noodzaak tot harmonisatie van zorgplichten in EU-verband en internationaal verband op te starten. De CSR heeft tijdens het forum de handreiking Zorgplichten als good practice gedeeld. Vanuit verschillende perspectieven is een bijdrage geleverd aan de discussie (industrie, consumenten, juridisch oogpunt). Het belang van het onderwerp zorgplichten werd door de deelnemers gedeeld en de bereidheid is er om het onderwerp in IGF-verband verder te brengen. Ter voorbereiding op de sessie in Genève heeft de CSR tijdens het NL IGF event in oktober van dit jaar met Nederlandse deelnemers van gedachten gewisseld over dit onderwerp. De uitkomsten uit deze sessie (behoefte aan wereldwijde best practices, toepassen multistakeholder-model en gebruikmaken van huidige wetgeving) stonden centraal tijdens de sessie op het IGF in Genève.





## 5. OVERIGE ADVIEZEN EN ACTIVITEITEN

De Cyber Security Raad (CSR) voerde in 2017 ook een aantal algemene activiteiten uit die hebben bijgedragen aan een open, veilig en welvarend digitaal Nederland. Zo hebben raadsleden hun medewerking verleend aan evenementen, heeft de raad zelf in samenwerking met andere organisaties een aantal evenementen georganiseerd, zijn boardroomgesprekken gevoerd en is de media benaderd om diverse onderwerpen over cybersecurity voor het voetlicht te brengen.

### Ondertekening brief Verhagen aan informateur

In maart 2017 heeft Herna Verhagen, CEO PostNL en auteur van het rapport 'De economische en maatschappelijke noodzaak van meer cybersecurity – Nederland digitaal droge voeten' een brief gestuurd aan voormalig informateur Edith Schippers. De CSR heeft deze brief mede ondertekend. Volgens Verhagen is krachtige sturing vanuit de overheid nodig. Daarom riep zij in deze brief het nieuwe kabinet op om cybersecurity, als cruciaal onderdeel van de digitaliseringsslag, te verstevigen door middel van een meerjarig actieprogramma. Deze oproep deed zij mede namens Eelco Blok (CEO KPN), Ference Lamp (Managing Director and Country executive Benelux Bank of America Merrill Lynch), Jeroen de Haas (CEO Eneco Group), Jos Nijhuis (President en CEO Schiphol Group), Wiebe Draijer (CEO Rabobank), Daniel Ropers (CEO bol.com) en de CSR.

### VenJ iTour

Ook tijdens de VenJ iTour in april 2017 heeft de CSR in april dit jaar aandacht gevraagd voor cybersecurity. De VenJ iTour is het jaarlijkse ontmoetingsmoment voor iBestuurders, iProfessionals en iPartners in het JenV-domein. Tijdens een paneldiscussie met Lotte de Bruijn, directeur ICT Nederland, Ad Reuijl, directeur Centrum Informatiebeveiliging en Privacy en Ronald Verbeek, directeur CIO Platform Nederland, is gesproken over onder andere het belang van cybersecurity in de boardroom, digitale zorgplichten van leveranciers en cyberhygiëne. Een verslag van de paneldiscussie is te lezen in de [congreskrant VenJiTour \(vanaf pagina 27\)](#).





## Cybersecurity aan de formatietafel - Debat met Tweede Kamerleden

Herna Verhagen, de CSR en ECP hebben in april 2017 een live debat over cybersecurity georganiseerd met Tweede Kamerleden Kees Verhoeven (D66), Mustafa Amhaouch (CDA) en Sven Koopmans (VVD), onder leiding van moderator Roelof Hemmen. Herna Verhagen, CEO PostNL en auteur van het rapport 'De economische en maatschappelijke noodzaak van meer cybersecurity – Nederland digitaal droge voeten' wilde met het debat een beweging op gang brengen. Tijdens het debat is over verschillende onderwerpen gesproken, waaronder thema's als politieke prioriteit voor cybersecurity, publiek-private samenwerking en cybersecurity als onderwerp voor regeerakkoord. Een verslag van dit symposium is terug te lezen op de [website van de CSR](#). Ook via [Youtube](#) is het debat terug te zien.

## Symposium 'Grip op cybersecurity'

In mei 2017 organiseerde iBestuur samen met de CSR een symposium met als titel 'Grip op cybersecurity'. Belangrijkste boodschap van het symposium was dat onze informatie een ronduit zorgelijk beeld van cyberdreigingen toont. Bestuurders hebben geen enkel excuus meer om de digitale dreiging te onderschatten. Het is een onderwerp dat op de bestuurstafel thuisheert. Een verslag van dit symposium is terug te lezen op de [website van de CSR](#).

## Working Dinner

Voorafgaand aan de ONE Conference in mei 2017 hebben de CSR en de Nationaal Coördinator Terrorismedebat en Veiligheid (NCTV) een 'working dinner' georganiseerd. Dertig genodigden uit het cybersecurityveld waren hiervoor uitgenodigd. De opening werd verzorgd door Jos Nijhuis, CEO Schiphol en raadslid van de CSR gevolgd door drie sprekers, te weten Melissa Hathaway, leading expert in cyberspace policy and cybersecurity, Michael Waksman, CEO at Jetico en Daniel Castro, vice president Information Technology and Innovation Foundation (ITIF). Daarna hebben aan tafel inhoudelijke discussies plaatsgevonden over diverse onderwerpen gerelateerd aan cybersecurity, zoals cybersecurity in het onderwijs, het dreigende tekort aan cybersecurity-experts, het belang van publiek-private samenwerking en de leidende rol van de overheid. Ook het rapport van Melissa Hathaway 'The Netherlands cyber readiness at a glance' is besproken. Patrica Zorko van de NCTV heeft het diner afgesloten.

## Cyber Security Beeld Nederland (CSBN) 2017

In juni 2017 is het CSBN 2017 gepubliceerd. De CSR heeft naar aanleiding hiervan een [persbericht](#) uitgebracht met een reactie op de inhoud ervan. Samenvattend herkent de raad het beeld dat op digitaal gebied steeds meer veiligheidsmaatregelen worden genomen, maar dat Nederland de opkomst van nieuwe technologieën en bijbehorende kwetsbaarheden nog niet kan bijbenen. Met name Internet of Things baart de raad zorgen.

## Cybersecurity Week HSD

In september 2017 vond in Den Haag de tweede editie van de internationale Cyber Security Week van The Hague Security Delta (HSD) plaats. Tijdens het openingsdebat heeft Jos Nijhuis als covoorzitter van de raad een inhoudelijke bijdrage geleverd om de urgentie van cybersecurity te benadrukken. Een van de onderwerpen die tijdens het debat behandeld werd was het rapport dat Deloitte heeft gepubliceerd, getiteld '[Dealing efficiently with cybercrime | Cyber Value at Risk in The Netherlands](#)'. Het rapport bevat informatie over de economische schade voor Nederlandse bedrijven en overheden door cybercrime.

## Big 4 en M7 cyberontbijten (Schiphol en Bureau Secretaris)

Jos Nijhuis, CEO Schiphol Group, organiseert namens de Cyber Security Raad BIG 4 cyberontbijten (EY, PwC, KPMG en Deloitte) en M5 cyberontbijten (BDO, Grant Thornton, Baker Tilly Berk, Accon avm en Mazars). Doel van de bijeenkomsten is om te bezien wat de accountancybranche in Nederland kan doen om meer awareness voor cybersecurity te creëren. Dit is in het kader van maatschappelijk verantwoord ondernemen en groot helpt klein (follow-up rapport Verhagen). Daarbij wordt zoveel als mogelijk de aansluiting gezocht bij bestaande initiatieven. In 2017 hebben de eerste cyberontbijten plaatsgevonden en ook in 2018 staan er cyberontbijten voor BIG 4 en M5 op de planning.

Om het belang van cybersecurity onder de aandacht te brengen heeft de CSR ook een boardroom-gesprek gehouden met de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) en heeft Jos Nijhuis gesproken op de Landelijke Jaardag van de NBA in november 2017.



## Boardroommeetings

In 2017 hebben de leden van de CSR ook boardroomgesprekken gevoerd. Organisaties worden op basis van vrijwilligheid door de leden bezocht. Het doel is de awareness voor cybersecurity op strategisch niveau te verhogen. De focus lag in 2017 op zowel brancheorganisaties als de medische sector. Er zijn boardroomgesprekken gevoerd bij de Nederlandse Beroepsorganisatie van accountants (NBA), MBO-Raad, Koninklijke Notariële Beroepsorganisatie (KNB), Zorgverzekeraars Nederland (ZN), VO-Raad, Vereniging van waterbedrijven in Nederland (Vewin), DC Klinieken en de Nederlandse Vereniging van Ziekenhuizen.

## CSR in de Media

In het afgelopen jaar heeft de CSR zelf actief de media benaderd om aandacht te creëren rondom belangrijke thema's voor cybersecurity. Zo is er veel aandacht besteed aan de publicatie van het CSR Magazine, de Handreiking Zorgplichten en het uitbrengen van het advies over informatie-uitwisseling. Ook is een column van de nieuwe covoorzitter Jos Nijhuis verschenen in de speciale uitgave '[Digitalisering van de publieke sector](#)' van Pulse Media Group. Hierin schrijft hij vooral over de voorbeeldrol die overheden en medeoverheden hebben in de digitalisering van onze samenleving. Eind december heeft de organisatie NLO een nieuwe editie van haar [relatiemagazine Fortify](#) gepubliceerd. In deze uitgave is een interview te lezen met prof. mr. Lokke Moerel, Senior Of Counsel Morrison & Foerster LLP, Hoogleraar Global ICT Law Universiteit Tilburg en lid van de CSR. In het interview gaat Lokke Moerel in op de kansen en bedreigingen op het vlak van cybersecurity, de verantwoordelijkheden ofwel zorgplichten die bedrijven hiertoe hebben en wat bedrijven kunnen doen om risico's te minimaliseren, ook gerelateerd aan Intellectueel Eigendom. "Informatie over innovaties die met het octrooibureau wordt uitgewisseld, dat is een heel interessant kanaal om op in te tappen", aldus Lokke Moerel.



